REMARKS

Claims 1-10 are pending. Claim 1 has been amended, claim 6 has been cancelled, and new claims 19-21 are added with this response. Claims 11-18 were previously cancelled with the prior response. Reconsideration of the application is respectfully requested for at least the following reasons.

I. REJECTION OF CLAIMS 1-6, 8, AND 9 UNDER § 102

Claims 1-6, 8, and 9 were rejected under 35 U.S.C. §102(e) as being clearly anticipated by U.S. Patent Publication No. 2004/0062267 (Minami et al.). Withdrawal of the rejection is respectfully requested for at least the following reasons.

Claim 1 of relates to a network interface system comprising a security system having first and second processors for encrypting outgoing data, wherein the first and second processors each comprise pipelines for ESP encryption, ESP authentication, and AH authentication. The Office Action alleges that Minami et al. thoroughly teach pipelines throughout the reference, in particular citing paragraphs 1744-1746, 105, 896, 1605-1622. (*See*, *O.A. dated 09/26/08*, p. 5, lns. 3-5). However, it is respectfully argued that ***Minami et al. fail to anticipate pipelining,*** as will be more fully appreciated below.

The Advisory Action describes pipelining as, "[i]n parallel processing, a method in which instructions are passed from one processing unit to another, as on an assembly line, and each unit is specialized for performing a particular type of operation." (*See*, *Advisory Action dated 12/11/08*). In other words, ***pipelining comprises a set of separate data processing elements, connected in series, so that the output of one element is the input of the next.*** For example, in one non-limiting embodiment, a processor comprising pipelines would have an encapsulating security payload (ESP) authentication engine, which operates on data and is configured to output the data to an authentication header (AH) engine, which operates on the data and is configured to output the data to an ESP encryption engine which operates on the data. Therefore, the process acts as an assembly line wherein separate processing elements perform separate processing functions.

Minami et al. do teach an encryption-authentication module 674 that may comprise two parallel encryption engines and therefore it is conceded that Minami et al. teach parallel processing. ***However, Minami et al. do not anticipate separate data processing elements for authentication and encryption*** as required for pipelines.

In particular, paragraph [0105] and [0896] of Minami et al. mention ESP, but ***do not anticipate or provide any indication of the use of pipelining*** (*i.e.,* do not mention the use of separate data processing elements, connected in series, so that the output of one element is the input of the next).

Paragraphs [1591] through [1622] relate to an IPSEC support architecture with a memory structure having separate blocks for storing AH and ESP protocols. The IPSEC support structure ***only teaches separate blocks <u>for storing protocols in memory</u>*** and specifically states that it "assumes ***a separate module*** to handle ***the computational aspects*** of encryption, decryption, and authentication functions of the protocol." (*See*, par. [1593])(emphasis added). Please note that paragraph 1593 specifically uses a singular noun to reference the separate module handling the computational aspects of encryption and authentication. Therefore, paragraphs [1591] through [1622] teach a ***single separate module*** to handle computational aspects of encryption and decryption, but do not anticipate or indicate the use of pipelining (*i.e.,* do not use separate data processing elements, connected in series, so that the output of one element is the input of the next).

Paragraphs [1744] through [1746] relate to an encryption /authentication engine. The encryption/authentication engine is illustrated in Fig. 67 as a single encryption-authentication engine 674. In regard to the single encryption-authentication engine 674 Minami et al. state that "[t]his module 674 is responsible for encrypting and adding authentication to a packet." (*See*, par. [1745]). Therefore, ***a <u>single module</u> 674 is responsible for <u>both encryption and authentication</u>*** and there is no indication of separate processing elements as required for pipelining.

Accordingly, all of the cited sections of Minami et al. are ***silent with respect to separate processing elements*** for encryption and authentication as required for pipelining, and in opposition to pipelining ***Minami et al. teach a single module for encryption and authentication.*** Therefore, Minami et al. fail to anticipate over claim 1 of the present invention and withdrawal of the rejection is respectfully requested.

Claims 2-5, 8, and 9 depend upon claim 1 and add further limitations thereto. Because Minami et al. do not anticipate the present invention of claim 1, claims 2-5, 8, and 9 are not anticipated by the cited art. Accordingly, withdrawal of the rejection is respectfully requested.

II. REJECTION OF CLAIMS 4 AND 5 UNDER 35 U.S.C. § 103

Claims 4 and 5 were rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent Publication No. 2004/0062267 (Minami et al.). Withdrawal of the rejection is respectfully requested for at least the following reasons.

As stated above, Minami et al. do not anticipate the invention of independent claim 1. Claims 4 and 5 depend upon claim 1 respectively, and adds further limitations thereto. Because the primary reference does not teach over the present invention of claim 1, claims 4 and 5 are also non-obvious over the cited art. Accordingly, withdrawal of the rejection is respectfully requested.

III. REJECTION OF CLAIM 7 UNDER 35 U.S.C. § 103(a)

Claim 7 was rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent Publication No. 2004/0062267 (Minami et al.) in view of U.S. Patent Publication 2004/0128553 (Buer et al.). Withdrawal of the rejection is respectfully requested for at least the following reasons.

As stated above, Minami et al. do not anticipate the invention of independent claim 1. Claim 7 depends upon claim 1, and adds further limitations thereto. Because the primary reference does not teach over the present invention of claim 1, and because Buer et al. fail to remedy the deficiencies in the primary reference, claim 7 is also non-obvious over the cited art. Accordingly, withdrawal of the rejection is respectfully requested.

IV. REJECTION OF CLAIM 10 UNDER 35 U.S.C. § 103(a)

Claim 10 was rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent Publication No. 2004/0062267 (Minami et al.) in view of Patt , Patel, Evers, Friendly, and Start's "One Billion Transistors, One Uniprocessor, One Chip" (Patt et al.). Withdrawal of the rejection is respectfully requested for at least the following reasons.

As stated above, Minami et al. do not anticipate the invention of independent claim 1. Claim 10 depends upon claim 1, and adds further limitations thereto. Because the primary reference does not teach over the present invention of claim 1, and because Patt et al. fail to remedy the deficiencies in the primary reference, claim 10 is also non-obvious over the cited art. Accordingly, withdrawal of the rejection is respectfully requested.

V. NEW CLAIMS 19-21

Claim 19 relates to a network interface system comprising a transmit output data flow controller configured to control the flow of encrypted data from first and second processors to a memory system in the same order as the order in which the data was read from the memory system. Minami et al. fail to teach a transmit output data flow controller configured to control the flow of encrypted data from the first and second processors to the memory system ***in the same order as the order in which the data was read from the memory system.***

Minami et al. teach a security system comprising two parallel and identical encryption engines. (*See,* par. [1746]). Packets are transferred from a memory to the security system, where the encryption engines are "serviced in alternating order". (*See,* par. [1746]). Once serviced, the encrypted packet is written back ***to the same memory location that the source packet came from***. (*See,* par. [1745]). Therefore, as taught by Minami et al., after encryption, packets are written to a memory ***location based***

upon the location from which they were read. In contrast, claim 19 relates to a transmit output data flow controller configured to write data to a memory location ***based upon the order in which it was read.*** Therefore, Minami et al. fail to teach over the transmit output data flow controller recited in claim 19. Accordingly, claim 19 is patentably distinct over the cited art.

New claim 20 relates to a network interface system comprising a memory system comprising a first memory coupled with a bus interface system and a security system for storage of outgoing data prior to encryption and incoming data after decryption and a second memory coupled with a media access control system and the security system for storage of incoming data prior to decryption and outgoing data after encryption, wherein the first and second memories comprise different memory locations. Minami et al. ***fail to teach a memory system comprising a first memory configured to store unencrypted data associated with the encryption and decryption engines and a second, separate, memory configured to store encrypted data associated with the encryption and decryption engines.***

As stated above, Minami et al. teach a security system, wherein packets are transferred from a memory to the security system, where the encryption engines are "serviced in alternating order". (*See,* par. [1746]). Once serviced the encrypted data is written back to the same memory location that the source packet came from. (*See,* par. [1745]). Therefore, as taught by Minami et al. ***a single memory location stores encrypted and unencrypted packets associated with the decryption engine and a separate single memory location stores encrypted and unencrypted packets associated with the encryption engine***.

In contrast, claim 20 relates to a network interface system comprising a first memory location for unencrypted data for ***both the encryption and decryption engines*** and a second, separate, memory location for encrypted data ***for both the encryption and decryption engines***. Therefore, the structure of memories recited in claim 20 is different than that taught by Minami et al. Accordingly, new claim 20 is patentably distinct over the cited prior art.

Claim 21 relates to a network interface system comprising a memory system comprising a unitary memory system partitioned into first and second memory areas. For the same reasons stated above in regard to claim 20, Minami et al. fail to teach unitary memory system partitioned into first and second memory areas. Accordingly, new claim 21 is patentably distinct over the cited prior art.

VI. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, AMDP751US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600